(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 083 722 A2

(12) EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
14.03.2001 Patentblatt 2001/11

(51) Int Cl.[7]: **H04L 29/06**, H04L 12/22, H04Q 7/32

(21) Anmeldenummer: **00810028.1**

(22) Anmeldetag: **12.01.2000**

(84) Benannte Vertragsstaaten:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Benannte Erstreckungsstaaten:
AL LT LV MK RO SI

(30) Priorität: **07.09.1999 US 152356 P**

(71) Anmelder: **Swisscom AG**
3050 Bern (CH)

(72) Erfinder:
- **Huber, Adriano**
  6600 Locarno (CH)
- **Loher, Urs, Dr.**
  3072 Ostermundigen (CH)

(74) Vertreter: **Saam, Christophe**
Patents & Technology Surveys SA
P.O. Box 1448
2001 Neuchâtel (CH)

(54) Verfahren, System und Gateway, die einen End-zu-End gesicherten Zugriff auf WAP-Dienste erlauben

(57) Verfahren, mit welchem ein Mobilteilnehmer mit einem WAP-tauglichen Endgerät (1) auf einen WAP oder WEB-Server (5) zugreifen kann,
wobei das benannte Endgerät (1) eine Anfrage für den benannten Server an ein WAP-Gateway (3) sendet,

wobei die Sicherheit in der Luftschnittstelle (2) zwischen dem benannten WAP-tauglichen Endgerät (1) und dem benannten Gateway (2) auf WTLS (Wireless Transport Layer Security) basiert,
wobei der benannte Server (5) mit dem SSL und/oder TLS Sicherheitsprotokoll gesichert ist,
wobei die Konversion zwischen WTLS und SSL und/oder TLS in einem vom Verwalter des benannten Servers (5) verwalteten gesicherten Gebiet erfolgt,
und wobei die Pakete, die vom benannten Endgerät (1) gesendet werden, vom benannten Gateway (3) zum benannten gesicherten Gebiet weitergeleitet werden, ohne dass alle Pakete die während einer Session übertragen werden entschlüsselt werden.

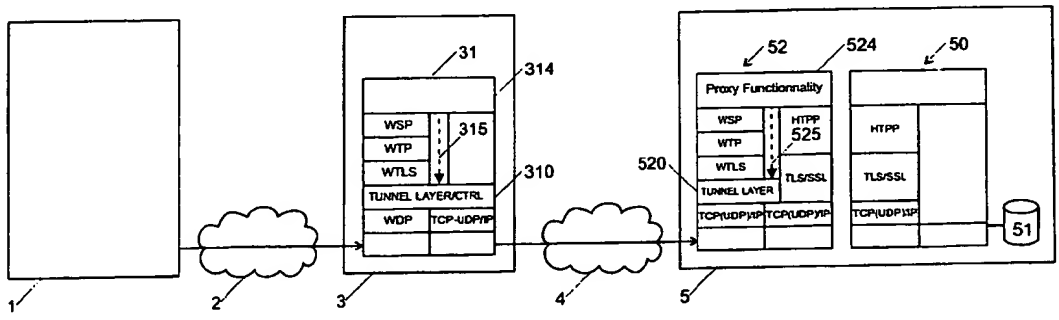

Fig. 3

EP 1 083 722 A2

Beschreibung

[0001] Die vorliegende Erfindung betrifft ein Verfahren, mit welchem ein Mobilteilnehmer mit einem WAP-tauglichen Endgerät auf einen WAP oder WEB-Server zugreifen kann.

[0002] WAP (Wireless Application Protocol)-Server, welche WAP basierte Dienste zur Verfügung stellen, sind an sich schon bekannt. Insbesondere sind auf WAP-basierte Dienste im Bereich von e-commerce und von finanziellen Instituten erhältlich.

[0003] Solche Dienste verlangen eine gesicherte Paketübertragung zwischen den Endbenutzern und dem Server des Dienstanbieters. Die gewöhnliche und vom WAP-Forum empfohlene Lösung verwendet die WTLS-Protokollschicht (Wireless Transport Layer Security); dieses Verfahren kann jedoch nur zum sichern der Paketübertragung zwischen den Endgeräten und einem (beispielsweise vom Mobilfunknetzbetreiber verwalteten) Gateway verwendet werden. In diesem Gateway wird eine Protokollübersetzung zum Sicherheitsprotokoll SSL 3.1 oder zum TLS 1.0 durchgeführt.

[0004] Das Prinzip einer mit diesem Verfahren gesicherten Datenübertragung ist schematisch auf der Figur 2 dargestellt. Mit dem Bezugszeichen 1 ist ein WAP taugliches Endgerät, beispielsweise ein WAP-taugliches GSM-Mobilfunktelefon (Global System for Mobile Communication) dargestellt, das sich über ein digitales Mobilfunknetz 2 mit einem vom Betreiber dieses Netzes verwalteten Gateway verbinden kann. Das Endgerät 1 enthält ein Browser. Mit 5 ist ein Server eines Dienstanbieters, beispielsweise eines Finanzinstituts oder eines Anbieters im e-commerce Bereich, dargestellt. Dieser Server kann auf eine Datenbank 51 zugreifen, in welcher WEB und/oder WAP-Seiten gespeichert sind. Die WEB oder WAP-Seiten können beispielsweise HTML-, WML-, JAVA-Script-, WML-Script-, usw., Dokumente enthalten.

[0005] Der Benutzer des Endgeräts 1, der auf eine WEB-oder WAP-Seite in der Datenbank 51 zugreifen kann, muss zu diesem Zweck eine mit WTLS-Diensten gesicherte Anfrage durch das Gateway 3 zum Server 5 senden. Diese Anfrage wird im Gateway 3 durch alle Protokollschichten eines Konvertierungsmoduls 30 entschlüsselt, und dann in eine mit TLS oder SSL gesicherte Anfrage übersetzt, die über ein TCP/IP Netz 4 an den Server 5 gesendet wird. Im Server 5 kann ein anderes Übersetzungsmodul vorgesehen werden, das diese Anfrage in ein eigenes Format konvertiert, welches vom Datenbankverwaltungssystem 51 verstanden werden kann. Die Antwort vom Server 5, beispielsweise der Inhalt einer WEB oder WAP-Seite, wird in der anderen Richtung über das Gateway 3, wo es umkonvertiert wird, zum Endgerät 1 geleitet.

[0006] Dieses Verfahren erlaubt keine echte End-zu-End Verschlüsselung; Daten und Pakete müssen im Gateway 3 entschlüsselt und wieder verschlüsselt werden, damit die Protokollübersetzung durchgeführt wird. Für viele Anwendungen ist eine solche Sicherheitslücke jedoch nicht akzeptierbar.

[0007] Ein Ziel der vorliegenden Erfindung ist es, ein neues sichereres Datenübertragungsverfahren zwischen einem Endgerät und einem WAP oder WEB-Server anzubieten.

[0008] Ein anderes Ziel ist es, ein neues Verfahren anzubieten, mit welchem eine End-zu-End gesicherte Verbindung zwischen einem WAP-tauglichen Endgerät und einem WAP oder WEB-Server hergestellt werden kann.

[0009] Ein weiteres Ziel ist es, ein neues Verfahren anzubieten, welches mit jedem WAP-tauglichen Endgerät das WTLS verwendet, eingesetzt werden kann, insbesondere mit Endgeräten, die eine Serverauthentifizierung basierend auf einem RSA-Schlüssel, auf X.509v3 Zertifikaten, auf RC5 oder auf anderen Sicherheitsprotokollen gemäss WAP oder WTLS, bzw. auf weiteren digitalen Zertifikaten, verwenden.

[0010] Gemäss der vorliegenden Erfindung werden diese Ziele insbesondere durch die Merkmale der unabhängigen Ansprüche erreicht. Weitere vorteilhafte Ausführungsformen gehen ausserdem aus den abhängigen Ansprüchen und der Beschreibung hervor.

[0011] Insbesondere werden diese Ziele durch ein Verfahren erreicht, in welchem das benannte Endgerät eine Anfrage für den benannten Server an ein WAP-Gateway sendet, wobei die Sicherheit in der Luftschnittstelle zwischen dem benannten WAP-tauglichen Endgerät und dem benannten Gateway auf WTLS (Wireless Transport Layer Security) basiert, wobei der benannte Server eine SSL und/oder TLS Protokollschicht enthält, wobei die Konversion zwischen WTLS und SSL und/oder TLS in einem vom Verwalter des benannten Servers verwalteten gesicherten Gebiet erfolgt, und wobei die Pakete, die vom benannten Endgerät gesendet werden, vom benannten Gateway zum benannten gesicherten Gebiet weitergeleitet werden, ohne alle Pakete, die während einer Session übertragen werden, zu entschlüsseln.

[0012] Die Pakete werden durch eine sogenannten Tunnelschicht durch das Gateway übertragen, ohne dass sie entschlüsselt werden. Dadurch bleibt der Inhalt selbst dem Betreiber des Gateways unbekannt. Die Pakete werden dann erst beim Server des Dienstanbieters in einem Proxy (sogenannten E2ES-Proxy) entschlüsselt und mit dem Zertifikat einer vertrauten Drittinstanz verifiziert.

[0013] Ausserdem werden diese Ziele durch ein Verfahren erreicht, mit welchem ein Mobilteilnehmer mit einem WAP-tauglichen Endgerät auf einen WAP oder WEB-Server zugreifen kann, wobei das benannte Endgerät eine Anfrage für den benannten Server an ein WAP-Gateway sendet in welchem ein Browser im benannten Endgerät die Portnummer der beantragten WEB oder WAP-Seite extrahiert und in die zum benannten Gateway gesendeten Pakete

DOCID: <EP__1083722A2_I_>

kopiert, und in welchem die benannten Pakete im benannten Gateway in Abhängigkeit von dieser Portnummer weitergeleitet werden.

[0014] Ausserdem werden diese Ziele dadurch errecht, dass die Anfrage, die von einem Endgerät über ein Gateway an einen WEB oder WAP-Server gesendet wird, mit WTLS End-zu-End gesichert wird.

[0015] Vorzugsweise kann im Gateway zwischen Sessionen, die konventionell behandelt werden sollen und Sessionen, die gemäss der vorliegenden Erfindung weitergeleitet werden sollen, unterschieden werden.

[0016] Im Folgenden werden anhand der beigefügten Zeichnung bevorzugte Ausführungsbeispiele der Erfindung näher beschrieben:

[0017] Die Figur 1 vergleicht die Protokollschichten in einem WAP-Protokoll-Stapel und im Internet Protokoll-Stapel.

[0018] Die oben beschriebene Figur 2 zeigt das Prinzip einer gesicherten Datenübertragung gemäss dem normalen WAP-Protokoll.

[0019] Die Figur 3 zeigt das Prinzip einer gesicherten Datenübertragung gemäss einer ersten Variante der Erfindung.

[0020] Die Figur 4 zeigt das Prinzip einer gesicherten Datenübertragung gemäss einer zweiten Variante der Erfindung.

[0021] Die Figur 5 zeigt das Prinzip einer gesicherten Datenübertragung gemäss einer dritten Variante der Erfindung.

[0022] Die Figur 3 zeigt das Prinzip einer ersten Variante der Erfindung. Diese Figur zeigt ein in einem digitalen Mobilfunknetz 2 angemeldetes WAP-taugliches Endgerät 1, beispielsweise ein WAP-taugliches GSM-Mobilfunktelefon oder einen WAP-tauglichen tragbaren Rechner. Mit diesem Gerät kann ein Programm, beispielsweise ein WAP-Browser, ausgeführt werden, das sich als Kunde mit einem WAP und/ oder WEB-Server 5 verbinden kann und somit auf Daten in diesem Server zugreifen kann.

[0023] Der WAP- oder WEB-Server 5 enthält WML und/oder HTML-Seiten, die beispielsweise von einem Dienstanbieter (beispielsweise einem Finanzinstitut und/oder einem Anbieter im Bereich e-commerce) angeboten werden. Es wird oft von Dienstanbietern und Endbenutzern gewünscht, dass die Session die aufgebaut wird wenn ein Benutzer auf mehrere Seiten zugreift, gesichert wird. Insbesondere ist es oft nötig, dass manche Daten, die in beiden Richtungen zwischen dem Endgerät 1 und dem Server 5 übertragen werden, End-zu-End gesichert werden und dass keine Drittpartei, nicht einmal der Mobilfunknetzbetreiber, diese Daten entschlüsseln kann. Ausserdem wird eine gegenseitige Authentisierung des Dienstanbieters und des Mobilbenutzers benötigt.

[0024] Der Benutzer des Endgeräts kann eine gesicherte Seite erreichen, beispielsweise um eine Transaktion durchzuführen, indem er beispielsweise auf den entsprechenden URL einer gesicherten oder nicht gesicherten Seite klickt. Der vom Dienstanbieter definierte URL der Seite kann beispielsweise http://www.sp1.com:50443 lauten, wobei http://www.sp1.com die URL-Adresse des Dienstanbieter und 50443 seine Portnummer ist. In Wap werden hingegen die fortlaufenden Portnummerbereiche 920x angewendet.

[0025] Erfindungsgemäss werden die URL in den WML und/oder HTML-Seiten der Dienstanbieter so verfasst, dass die gewünschte Sessionsart (End-zu-End gesichert, Standard gesichert oder ungesichert) aus diesem URL, unter anderem aus der URL-Adresse und/oder aus der Portnummer, ermittelt werden kann.

[0026] Mit dem Bezugszeichen 3 ist ein ebenfalls dem Mobilfunknetz 2 angeschlossenes Gateway dargestellt. Das Gateway nimmt die Pakete vom Benutzer 1 entgegen und entschlüsselt das oder die ersten Pakete in jeder Session, bis eine Anwendung 314 die Portnummer und die URL der gewünschten WEB oder WAP-Seite aus den Paketen extrahieren kann.

[0027] Sobald diese Angaben gefunden worden sind, bestimmt die Anwendung 314 anhand den vom Verwalter des Gateways angegebenen Angaben, wie die Pakete bearbeitet werden sollen. Insbesondere bestimmt die Anwendung, ob die Session zwischen dem Endgerät 1 und dem Server 5 End-zu-End gesichert werden soll. Dies ist beispielsweise dann der Fall wenn sich die Portnummer (beispielsweise 50443) in einer vom Administrator des Gateways au[illegible]e bauten Liste befindet.

[0028] Das Gateway 3 verwendet eine zusätzliche Protokollschicht 310 (Tunnelschicht), die von der Anwendung 314 gesteuert wird (Pfeil 315). Wenn die Session gesichert werden soll, wird die Tunnelschicht 310 so gesteuert, dass alle nachfolgenden Pakete der Session in transparenter Art durch das Gateway geführt und an die Zieladresse des Servers 5 weitergeleitet werden, ohne konvertiert und vor allem ohne entschlüsselt zu werden.

[0029] Die immer noch mit WTLS gesicherten Pakete der Session werden dann über das Netz 4 weitergeleitet und vom Server 5 im gesicherten Gebiet des Dienstanbieters entgegengenommen. Das Netz 4 kann beispielsweise aus dem Internet oder aus einer gemieteten Telefon-Linie bestehen. Der Server 5 umfasst ein Proxy 52 welches später erläutert wird, ein konventionelles Gateway 50, und eine Datenbank 51, in welcher ein WEB- und/ oder WAP-Inhalt abgelegt ist.

[0030] Das Proxy 52 im Server 5 des Dienstanbieters wird so aufgebaut, dass es WTLS-gesicherte Sessionen entgegennehmen kann. Es umfasst vorzugsweise einen kompletten WAP-Protokoll-Stapel und kann somit durch vom Fachmann leicht durchführbare Anpassungen von standardisierter Software realisiert werden. In diesem Proxy werden empfangene mit WTLS gesicherte WDP-Datagramme mit dem Zertifikat einer vertrauten Drittinstanz geprüft, entschlüsselt und in normale TCP-IP-Datagramme übersetzt, wobei die HTTP-Session optional mit SSL gesichert werden

kann. Die TCP-IP konvertierten Pakete werden an den WAP- oder WEB-Server 50 weitergeleitet, der eventuell eine andere Protokollkonvertierung durchführt, damit die empfangene Abfrage vom Datenbanksystem 51 bearbeitet werden kann.

[0031] Als Alternative können die Datagramme mit einem Session-Schlüssel ver- und entschlüsselt werden, dssen Schlüssel mit Hilfe eines zertifizierten, öffentlichen Schlüssel während der Schlüsselvereinbarungsphase generiert werden.

[0032] Die Antwort vom WEB bzw. WAP-Server 50, zum Beispiel die gewünschte WEB- oder WAP-Seite, wird vom Server 50 in die andere Richtung gesendet, im Proxy 52 übersetzt und mit WTLS-Diensten gesichert und durch die "Tunnelschicht" 310 im Gateway 31 an das Endgerät 1 des Benutzers geleitet, wobei die gesamte Verbindung zwischen Server 5 und Endbenutzer 1 mit WTLS gesichert wird.

[0033] Datagramme, die aufgrund des enthaltenen URL und/oder Portnummer keine End-zu-End gesicherte Datenübertragung verlangen, werden im Gateway 31 gemäss der konventionellen vom WAP-Forum empfohlenen Lösung durch alle Schichten des Protokolls im Gateway 2 entschlüsselt, mit TLS/SSL wieder gesichert und an die in den Paketen angegebene URL-Adresse weitergeleitet. Beispielsweise werden Sessionen mit der Portnummer 80 wie gewöhnliche HTTP-Sessionen behandelt und weitergeleitet.

[0034] Antworten vom Server 5 (beispielsweise die gewünschten WEB oder WAP-Seiten) die keine WTLS-Sicherung zwischen Server und Gateway 3 verlangen, werden von der Proxy-Anwendung 524 durch eine Tunnelschicht 520 im Proxy durchgeführt (Pfeil 315) und erst im Gateway 3 mit WTLS-Diensten gesichert.

[0035] Diese Variante verlangt keine Änderungen vom Browser im Endgerät 11 und nur ein relativ einfaches Proxy 53 beim Dienstanbieter 5, das WTLS-Sessionen entgegennehmen kann. Die Software-Implementation des Gateways 3 kann sich jedoch als schwierig erweisen.

[0036] Die zweite Variante, die auf der Figur 4 dargestellt wird, erlaubt es, dieses Problem durch eine leicht durchführbare Anpassung der Anwendung (zum Beispiel des Browsers) im Endgerät 1 zu vermeiden. In dieser Variante wird die URL-Adresse und die Portnummer der verlangten WEB oder WAP-Seite vom Browser 10 in jedes Paket (WDP-Datagramm) der Session kopiert. Diese Pakete werden dann über das Mobilfunknetz 2 an das Gateway 3 gesendet, wo die Portnummer und die URL analysiert werden, um zu ermitteln wie die Pakete weiterbehandelt werden sollen.

[0037] Diese Variante hat den Vorteil, dass die Analyse und die Weiterbehandlung der Pakete in den unteren Schichten des Protokolls, unter anderem in der WDP und/oder WTLS-Schicht, durchgeführt werden kann und dass sie somit nur minimale Anpassungen des Gateways 3 verlangt.

[0038] Eine Tabelle 321 im Gateway 3 oder in einem nicht dargestellten Router vor dem Gateway gibt an, wie die Pakete je nach Portnummer und URL behandelt werden sollen und insbesondere welche Pakete transparent durch die Tunnelschicht 320 gehen sollen. Diese Tabelle kann vorzugsweise vom Administrator des Gateways 3 konfiguriert und geändert werden, ohne dass das Gateway neu gestartet werden muss, damit die Konfiguration während des Betriebes aktualisiert werden kann. Daten in der Tabelle können vorzugsweise nur vom Administrator geändert werden, oder von Personen mit Administratorenrechten.

[0039] Die Tabelle im Gateway 3 könnte beispielsweise folgende Zeilen enthalten:

	Eingegebene URL Adresse		Neue Adresse (vom Gateway erteilt)		Bemerkung
	Adresse	Portnummer	Adresse	Portnummer	
1	138.10.20.30	8040	140.50.60.70	12345	Pakete mit dieser Adresse werden auf transparente Weise an die neue Adresse geleitet. Die Portnummer wird ersetzt (Mapping).
2	*.*.*.*	50443	*.*.*.*	50443	Stern-Joker erlauben eine Bedingung für alle Server mit der gleichen Portnummer zu setzen
3	138.10.20.40	*	138.10.20.40	*	Wie oben, jedoch ohne DNS-Lookup
4	www.sp1.com	*	www.sp1.com	*	Alle URL vom sp1 müssen durch die Tunnelschicht
5	www.sp1.com	80	www.sp1.com	80	Alle Verbindungen mit Portnummer 80 durch die Tunnelschicht

DOCID: <EP__1083722A2_I_>

(fortgesetzt)

	Eingegebene URL Adresse		Neue Adresse (vom Gateway erteilt)		Bemerkung
	Adresse	Portnummer	Adresse	Portnummer	
6	www.sp1.ch	50443	www.sp1.ch	50443	sp1 verlangt, dass alle Sessionen mit der Portnummer 50443 durch die Tunnelschicht geleitet werden.
7	www.sp2.ch	443	www.sp2.ch	443	sp2 verlangt, dass alle Sessionen mit der Portnummer 443 durch die Tunnelschicht geleitet werden. Damit wird kein SSL mit dem Port 443 verwendet. SSL kann dann beispielsweise vom Proxy verwendet werden.
8	...				

[0040] Der Administrator des Gateways 3 wird vorzugsweise den Dienstanbietern einen Bereich von URL-Adressen und/oder Portnummern zur Verfügung stellen. Dienstanbieter SP1, SP2, usw. können dann eine oder mehrere URL, oder Portnummern, oder Kombinationen aus beiden, für sich reservieren und den Administrator 3 anweisen, Pakete mit dieser URL und/oder Portnummer transparent weiterzuleiten.

[0041] Die Figur 5 zeigt als Beispiel, wie die Pakete, die von verschiedenen Endbenutzern 1_1 bis 1_4 gesendet werden, vom Gateway 3 in Abhängigkeit ihrer URL-Adresse und/oder Portnummer behandelt werden.

[0042] Das dargestellte System umfasst in diesem Beispiel drei Server 5_1, 5_2 und 5_3 von drei verschiedenen Dienstanbietern sp1, sp2 und sp3. Die vier folgenden Seiten werden im ersten Server 5_1 (bzw. 5_2) abgelegt:

- eine ungesicherte WEB-Seite mit der Adresse www.sp1.com:80 (bzw. www.sp2.com:80)
- eine WEB-Seite mit der Adresse www.sp1.com:443 (bzw. www.sp2.com:443), die nur mit SSL gesichert wird (keine End-zu-End Sicherheit)
- eine WEB-Seite mit der Adresse www.sp1.com:50443 (bzw. www.sp2.com:50443), die mit WTLS gesichert wird (End-zu-End Sicherheit)
- eine WAP-Seite mit der Adresse wap.sp1.com:50443 (bzw. wap.sp2.com:50443), die mit WTLS gesichert wird (End-zu-End Sicherheit)

[0043] Im Server 5_3 des dritten Dienstanbieters sp3 werden nur zwei Seiten abgelegt:

- eine ungesicherte WEB-Seite mit der Adresse www.sp3.com:80
- eine WEB-Seite mit der Adresse www.sp3.com:443, die nur mit SSL gesichert wird (keine End-zu-End Sicherheit)

[0044] Der erste Benutzer 1_1 will auf die gesicherten Seiten www.sp1.com:443 und www.sp1.com:50443 des Dienstanbieters SP1 im Server 5_1 zugreifen, indem er GET(URL) Abfragen mit entsprechenden URL an das Gateway 3 sendet. Das Gateway 3 erkennt anhand der Tabelle 321 und des im Datagramm enthaltenen URL und/oder der Portnummer, welche Sicherheiten von diesen Seiten verlangt werden. Im ersten Fall (SSL Sicherheit) werden alle Datagramme der Session im Gateway 3 entschlüsselt und eine Übersetzung von WTLS zu SSL wird durchgeführt. Im zweiten Fall (End-zu-End Sicherheit mit WTLS) werden alle Datagramme der Session transparent an den Server 5_1 weitergeleitet, ohne dass sie entschlüsselt werden.

[0045] Der zweite Benutzer 1_2 will auf die Seite www.sp2.com:50433 des Dienstanbieters sp2 im Server 5_2 zugreifen, die eine End-zu-End Sicherheit verlangt. Datagramme mit dieser Adresse werden im Gateway 3 erkannt und transparent durch die Tunnelschicht an den Server 5_2 geleitet.

[0046] Der dritte Benutzer 13 will auf die Seite www.sp3.com:443 des Dienstanbieters sp2 im Server 5_2 zugreifen, die eine mit TLS/SSL gewährleistete Sicherheit verlangt. WTLS-gesicherte Datagramme mit dieser Adresse werden im Gateway 3 erkannt, durch alle Schichten des Protokoll-Stapels übersetzt, mit TLS/SSL gesichert und an den Server 5_3 weitergeleitet.

[0047] Der vierte Benutzer 1_4 will auf die ungesicherte Seite www.sp3.com:80 des Dienstanbieters sp2 im Server 5_2 zugreifen. WTLS-gesicherte Pakete mit dieser Adresse werden im Gateway 3 erkannt, durch alle Schichten des Protokoll-Stapels übersetzt und an den Server 5_3 weitergeleitet, ohne sie durch das Netz 4 zu sichern.

[0048] Diese Variante verlangt nur minimale Änderungen vom Gateway 3. Allerdings müssen die Browser-Anwendungen in den Endgeräten 1 leicht angepasst werden, was sich bei vielen Anbietern als schwierig erweisen kann.

[0049] Wir werden jetzt eine dritte Erfindungsvariante beschreiben, die diesen Nachteil vermeidet.

[0050] In dieser Variante werden Sessionen die eine End-zu-End Sicherheit verlangen anhand der URL-Adresse und/oder der Portnummer wie in der ersten oder zweiten Variante erkannt. Statt die Sessionen durch die Tunnelschicht transparent weiterzuleiten, sendet das Gateway in diesem Fall einen standardisierten Redirect-Befehl mit der in der Tabelle 321 angegebenen Adresse und Portnummer des Dienstanbieters und mit anderen Parameter für die Identifizierung vom Gateway 5, wie Dial-In Nummer, an das Endgerät 1.

[0051] Die Weiterleitungsadresse (Adresse, Portnummer, Dial-In Nummer, usw..) im Redirect-Befehl wird vorzugsweise aus einem vom WAP oder WEB-Server 5 zugänglich gemachten Dokument extrahiert. Der Redirect-Befehl kann auch dieses oder ein anderes Dokument oder die Adresse eines solchen Dokuments enthalten, in welchem die Weiterleitungsadresse enthalten ist. Im Dokument können vorzugsweise verschiedene Adressengebiete mit Stringmuster, beispielsweise mit *, angegeben werden.

[0052] Die Anwendung im Mobilgerät 1, die diesen Redirect Befehl entgegennimmt, reagiert, indem sie jetzt die schon vorher an das Gateway 3 gesendeten Pakete wieder direkt an die im Redirect-Befehl angegebene Adresse des Dienstanbieters sendet.

[0053] Alle Pakete in der Session werden dann direkt zwischen dem Endgerät 1 und dem Server 5 übertragen, bis der Endbenutzer einen anderen URL sendet, der vom Server 5 nicht bearbeitet werden kann (beispielsweise wenn sich die entsprechende gewünschte Seite nicht auf diesem Server befindet). In diesem Fall wird die Session vom Server 5 unterbrochen und die nachfolgenden Pakete werden wieder an das Gateway 3 gesendet.

[0054] Falls keine End-zu-End Sicherheit benötigt wird, wird kein Redirect Befehl vom Gateway 3 gesendet. In diesem Fall werden alle Pakete während der gesicherten Session durch das Gateway 3 gesendet.

Patentansprüche

1. Verfahren, mit welchem ein Mobilteilnehmer mit einem WAP-tauglichen Endgerät (1) auf einen WAP oder WEB-Server (5) zugreifen kann,
   wobei das benannte Endgerät (1) eine Anfrage für den benannten Server an ein WAP-Gateway (3) sendet,

   wobei die Sicherheit in der Luftschnittstelle (2) zwischen dem benannten WAP-tauglichen Endgerät (1) und dem benannten Gateway (3) auf WTLS (Wireless Transport Layer Security) basiert,
   wobei der benannte Server (5) mit dem SSL und/oder TLS Sicherheitsprotokoll gesichert ist,

   dadurch gekennzeichnet, dass die Konversion zwischen WTLS und SSL und/oder TLS in einem vom Verwalter des benannten Servers (5) verwalteten gesicherten Gebiet erfolgt,
   und dass die Pakete, die vom benannten Endgerät (1) gesendet werden, vom benannten Gateway (3) zum benannten gesicherten Gebiet weitergeleitet werden, ohne alle Pakete die während einer Session übertragen werden zu entschlüsseln.

2. Verfahren gemäss Anspruch 1, dadurch gekennzeichnet, dass das benannte Gateway (3) die benannten Pakete zu einem Proxy (52) im benannten gesicherten Gebiet weiterleitet, wobei das benannte Proxy (52) mindestens eine Protokollschicht des WAP-Protokolls verwendet.

3. Verfahren gemäss einem der Ansprüche 1 oder 2, in welchem die benannten Pakete in Abhängigkeit vom URI und/oder vom Domainname der angefragte Seite im benannten Gateway (3) weitergeleitet werden.

4. Verfahren gemäss einem der vorhergehenden Ansprüche, in welchem die benannten Pakete abhängig von der Portnummer im benannten Gateway (3) weitergeleitet werden.

5. Verfahren gemäss dem vorhergehenden Anspruch, in welchem die benannten Pakete abhängig von verschiedenen Portnummern an verschiedene gesicherte Gebiete weitergeleitet werden.

6. Verfahren gemäss einem der Ansprüche 4 oder 5, in welchem die benannte Portnummer aus der URI und/oder URL der angefragten Seite in einer Anwendungsschicht des benannten Gateways (3) extrahiert werden.

DOCID: <EP__1083722A2_I_>

7. Verfahren gemäss Anspruch 6, in welchem die benannte Portnummer während einer Session nur aus einer begrenzten Anzahl von Paketen extrahiert wird,
und in welchem das Weiterleiten von mindestens einem folgenden Paket von dieser benannten extrahierten Portnummer abhängig ist.

8. Verfahren gemäss Anspruch 7, in welchem ein Proxyserver (52) im benannten gesicherten Gebiet die URI und/oder die Portnummer der empfangenen Pakete extrahiert, und in welchem der benannte Proxyserver (52) dem benannten Gateway (3) einen Befehl zurücksendet, wenn er ein Paket mit einer anderen URI und/oder mit einer anderen Portnummer empfängt.

9. Verfahren gemäss einem der Ansprüche 4 oder 5, in welchem die benannte Portnummer aus dem benannten URI und/oder URL der angefragten Webseite im benannten Endgerät (1) extrahiert wird.

10. Verfahren gemäss Anspruch 9, in welchem die benannte Portnummer von einem Browser aus dem URI und/oder URL der angefragten Webseite extrahiert wird.

11. Verfahren gemäss einem der Ansprüche 8 oder 9, in welchem der Browser im benannten Endgerät (1) die benannte Portnummer in den benannten Paketen erst dann kopiert, wenn eine End-zu-End gesicherte Verbindung beantragt ist.

12. Verfahren gemäss einem der Ansprüche 3 bis 11, in welchem die benannten Pakete im benannten Gateway (3) an ein gesichertes Gebiet weitergeleitet werden wenn sich die benannte Portnummer in einem vorbestimmten Bereich befindet.

13. Verfahren gemäss Anspruch 1, dadurch gekennzeichnet, dass wenn eine End-zu-End gesicherte Verbindung beantragt ist, das benannte Gateway (3) einen Redirect-Befehl zum benannten Endgerät (1) sendet.

14. Verfahren gemäss dem vorhergehenden Anspruch, in welchem der benannte Redirect Befehl zeitlich begrenzt ist.

15. Verfahren gemäss Anspruch 13, in welchem ein Proxy Server (52) im benannten gesicherten Gebiet die URI und/oder die Portnummer der empfangenen Pakete extrahiert, und einen Redirect Befehl zurück zum benannten Endgerät (1) sendet, sobald die Session zum benannten Gateway (3) weitergeleitet werden soll.

16. Verfahren gemäss Anspruch 13, in welchem den benannten Redirect-Befehl eine Weiterleitungsadresse enthält, die aus einem vom benannten WAP oder WEB-Server (5) zugänglich gemachten Dokument extrahiert wird.

17. Verfahren gemäss dem Anspruch 13, in welchem den benannten Redirect-Befehl ein Dokument enthält, in welchem die Weiterleitungsadresse enthalten ist.

18. Verfahren, mit welchem ein Mobilteilnehmer mit einem WAP-tauglichen Endgerät (1) auf einen WAP oder WEB-Server (5) zugreifen kann,
wobei das benannte Endgerät (1) eine Anfrage für den benannten Server (5) an ein WAP-Gateway (3) sendet,
dadurch gekennzeichnet, dass ein Browser im benannten Endgerät (1) die Portnummer der beantragten WEB oder WAP-Seite extrahiert und in zum benannten Gateway (3) gesendete Paketen kopiert,
und dass die benannten Pakete im benannten Gateway (3) in Abhängigkeit von dieser Portnummer weitergeleitet werden.

19. Gateway (3), das mit WTLS-gesicherte Datagramme von WAP-tauglichen Endgeräten entgegennehmen und in SSL-gesicherte-Abfragen übersetzen kann,
dadurch gekennzeichnet, dass es Datagramme erkennen kann, die in transparenter Weise weitergeleitet werden sollen und dass es diese Datagramme ohne sie zu entschlüsseln weiterleiten kann.

20. Gateway gemäss dem vorhergehenden Anspruch, in welchem die benannten Pakete in Abhängigkeit vom URI und/oder vom Domainname der angefragten Seite weitergeleitet werden.

21. Gateway gemäss einem der Ansprüche 19 oder 20, in welchem die benannten Pakete in Abhängigkeit von der Portnummer im benannten Gateway (3) weitergeleitet werden.

SDOCID: <EP___1083722A2_I_>

22. Gateway gemäss dem vorhergehenden Anspruch, in welchem die benannten Pakete abhängig von verschiedenen Portnummern an verschiedene gesicherte Gebiete weitergeleitet werden.

23. Gateway gemäss einem der Ansprüche 21 oder 22, in welchem die benannte Portnummer aus dem URI und/oder URL der angefragten Seite in einer Anwendungsschicht des benannten Gateways (3) extrahiert werden.

24. Gateway gemäss Anspruch 21, in welchem die benannte Portnummer während einer Session nur aus einer begrenzten Anzahl von Paketen extrahiert werden,
und in welchem das Weiterleiten von mindestens einem folgenden Paket von dieser benannten extrahierten Portnummer abhängig ist.

DOCID: <EP__1083722A2_I_>

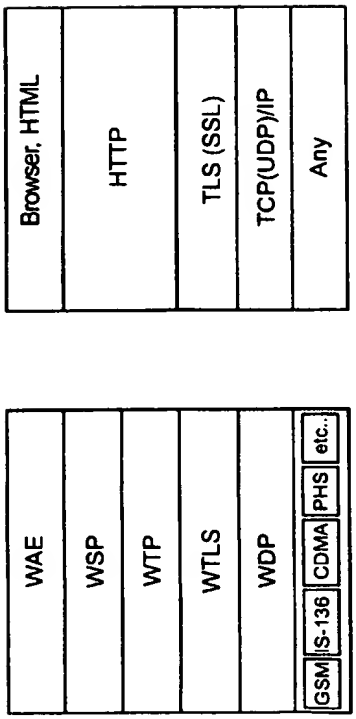

Fig. 1

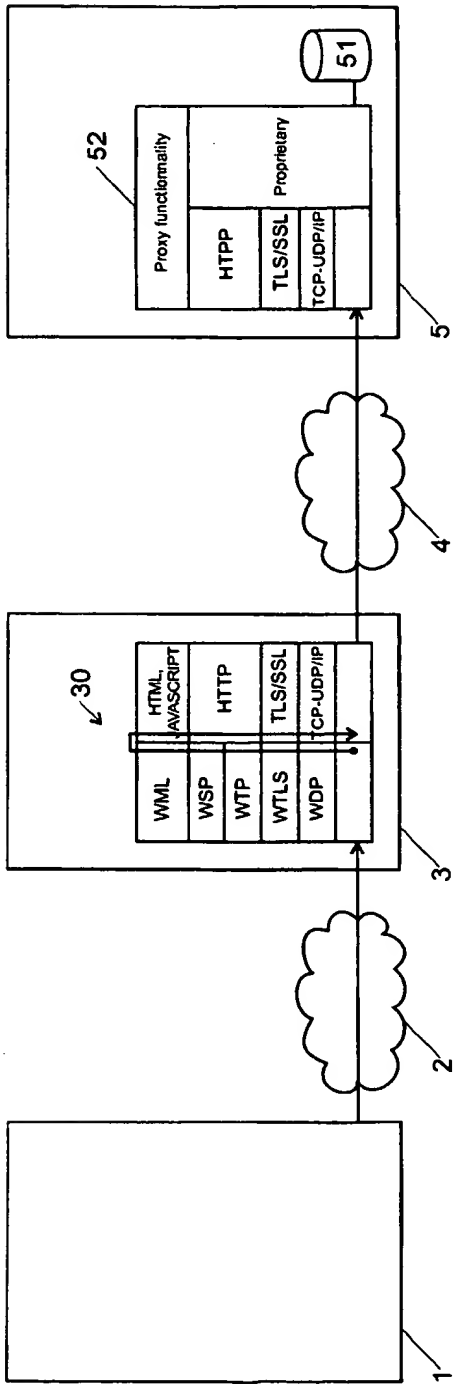

Fig. 2

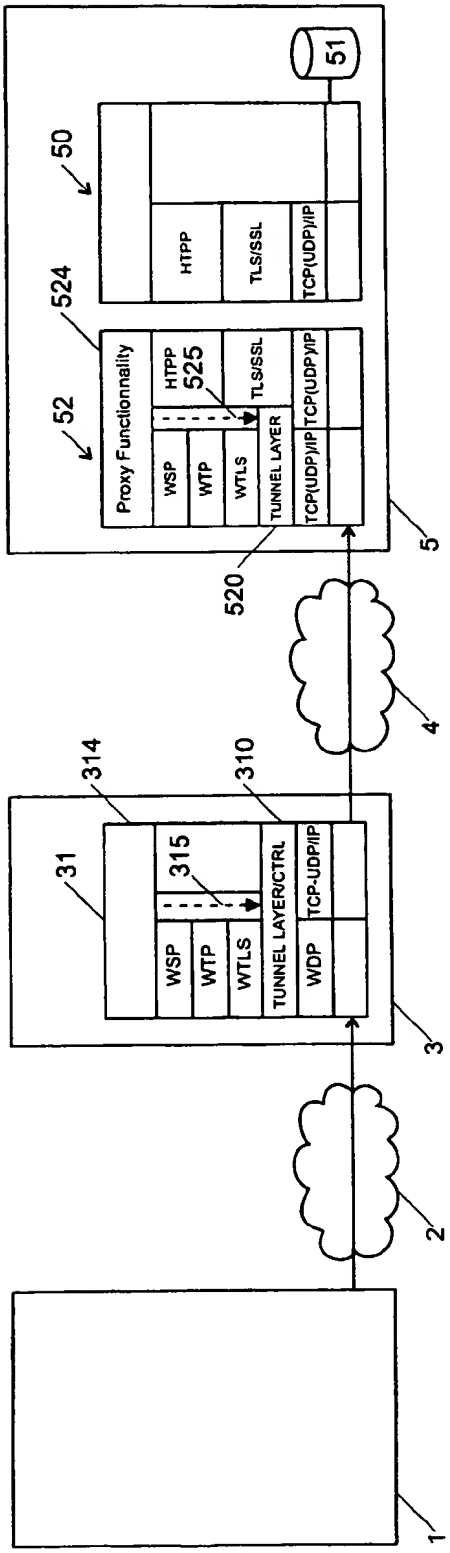

Fig. 3

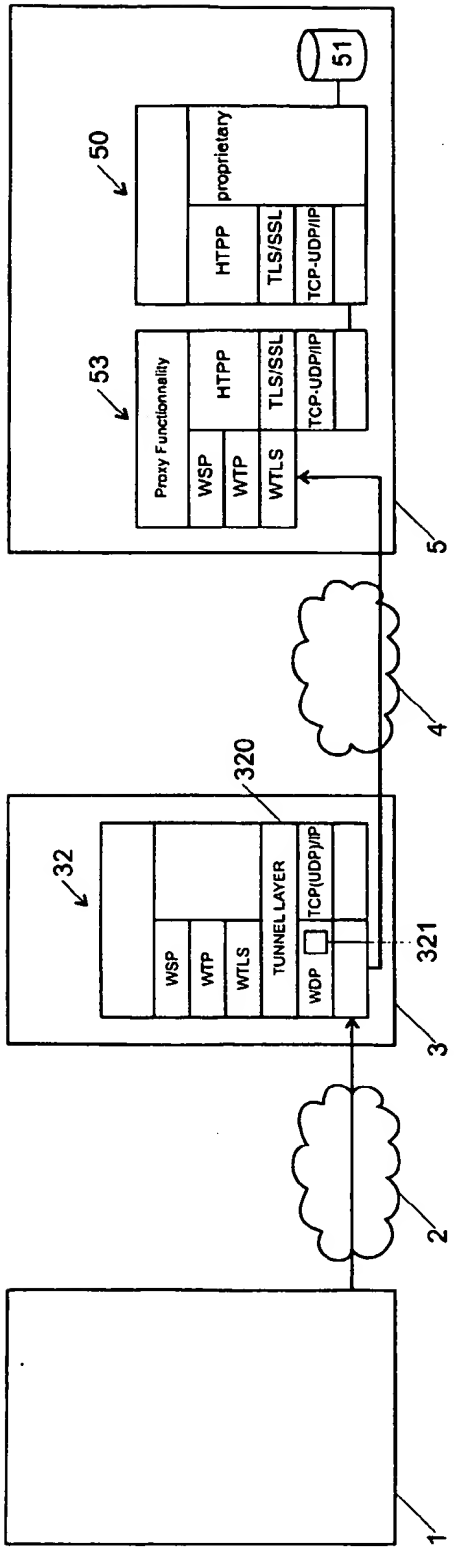

Fig. 4

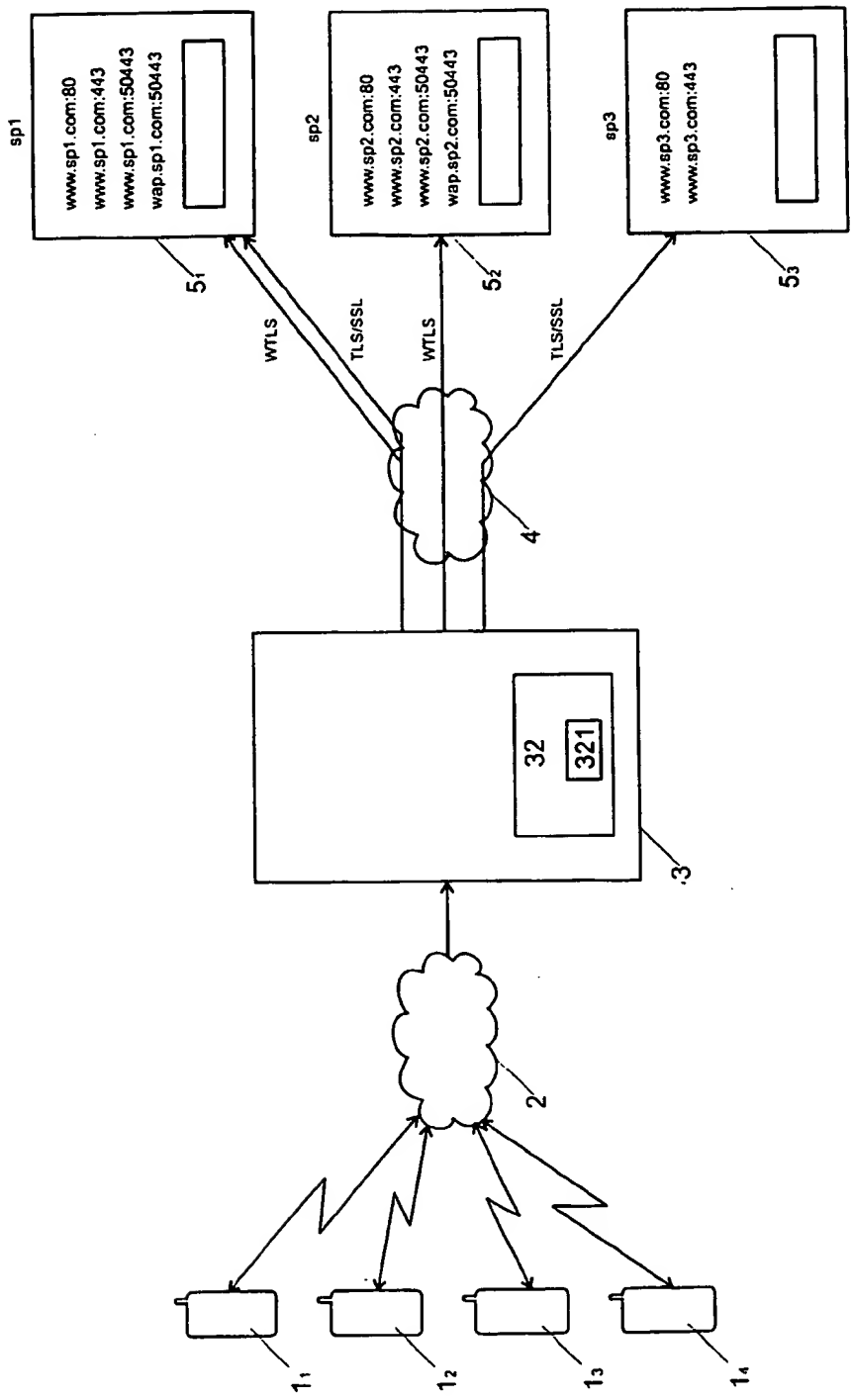

Fig. 5

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 083 722 A3

(12) EUROPÄISCHE PATENTANMELDUNG

(88) Veröffentlichungstag A3:
18.07.2001 Patentblatt 2001/29

(43) Veröffentlichungstag A2:
14.03.2001 Patentblatt 2001/11

(21) Anmeldenummer: **00810028.1**

(22) Anmeldetag: **12.01.2000**

(51) Int Cl.[7]: **H04L 29/06**, H04L 12/22, H04Q 7/32, H04L 29/08, H04L 12/56

(84) Benannte Vertragsstaaten:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Benannte Erstreckungsstaaten:
AL LT LV MK RO SI

(30) Priorität: **07.09.1999 US 152356 P**

(71) Anmelder: **Swisscom Mobile AG**
3050 Bern (CH)

(72) Erfinder:
- **Huber, Adriano**
  6600 Locarno (CH)
- **Loher, Urs, Dr.**
  3072 Ostermundigen (CH)

(74) Vertreter: **Saam, Christophe et al**
Patents & Technology Surveys SA
P.O. Box 1448
2001 Neuchâtel (CH)

(54) Verfahren, System und Gateway, die einen End-zu-End gesicherten Zugriff auf WAP-Dienste erlauben

(57) Verfahren, mit welchem ein Mobilteilnehmer mit einem WAP-tauglichen Endgerät (1) auf einen WAP oder WEB-Server (5) zugreifen kann,
wobei das benannte Endgerät (1) eine Anfrage für den benannten Server an ein WAP-Gateway (3) sendet,

wobei die Sicherheit in der Luftschnittstelle (2) zwischen dem benannten WAP-tauglichen Endgerät (1) und dem benannten Gateway (2) auf WTLS (Wireless Transport Layer Security) basiert,
wobei der benannte Server (5) mit dem SSL und/oder TLS Sicherheitsprotokoll gesichert ist,
wobei die Konversion zwischen WTLS und SSL und/oder TLS in einem vom Verwalter des benannten Servers (5) verwalteten gesicherten Gebiet erfolgt,
und wobei die Pakete, die vom benannten Endgerät (1) gesendet werden, vom benannten Gateway (3) zum benannten gesicherten Gebiet weitergeleitet werden, ohne dass alle Pakete die während einer Session übertragen werden entschlüsselt werden.

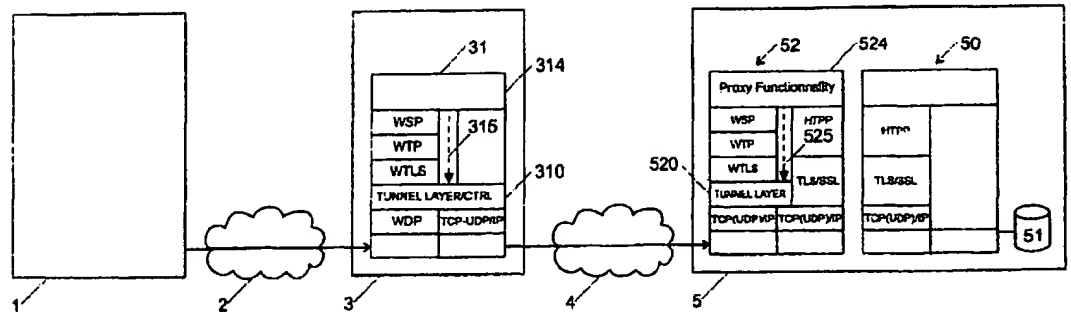

Fig. 3

EP 1 083 722 A3

Europäisches Patentamt

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 00 81 0028

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (Int.Cl.7)
P,A	WO 99 45684 A (NOKIA MOBILE PHONES LTD ;NYKAENEN PETRI (FI)) 10. September 1999 (1999-09-10) * Seite 11, Zeile 7 - Seite 13, Zeile 19 * * Seite 15, Zeile 16-19 *	1,18,19	H04L29/06 H04L12/22 H04Q7/32 H04L29/08 H04L12/56
A	& FI 980 485 A (NOKIA MOBILE PHONES LTD) 4. September 1999 (1999-09-04) * das ganze Dokument *	1,18,19	
A	LUOTONEN A: "Tunneling SSL Through a WWW Proxy" INTERNET DRAFT , 14. Dezember 1995 (1995-12-14), XP002167506 Internet Engineering Task Force (IETF) * das ganze Dokument *	1,18,19	
P,A	JORMALAINEN S AND LAINE J: "Security in the WTLS" SEMINAR ON NETWORK SECURITY, 'Online! 3. - 30. November 1999, XP002167503 Helsinki Gefunden im Internet: <URL:http://www.tml.hut.fi/Opinnot/Tik-110.501/1999/papers/wtls/wtls.html> 'gefunden am 2001-05-16! * Absatz '03.2! *	1,18,19	
P,O,A	-& HELSINKI UNIVERSITY OF TECHNOLOGY: "Seminar Program" SEMINAR ON NETWORK SECURITY, 'Online! 2. - 3. November 1999, Seite 03-11- XP002167504 Helsinki Gefunden im Internet: <URL:http://www.tml.hut.fi/Opinnot/Tik-110.501/1999/seminar.html> 'gefunden am 2001-05-16! * Absätze 'OIII!-'0002! *	1,18,19	

RECHERCHIERTE SACHGEBIETE (Int.Cl.7)

H04L

Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt

Recherchenort	Abschlußdatum der Recherche	Prüfer
DEN HAAG	23. Mai 2001	Dupuis, H

KATEGORIE DER GENANNTEN DOKUMENTE

X : von besonderer Bedeutung allein betrachtet
Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie
A : technologischer Hintergrund
O : nichtschriftliche Offenbarung
P : Zwischenliteratur

T : der Erfindung zugrunde liegende Theorien oder Grundsätze
E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist
D : in der Anmeldung angeführtes Dokument
L : aus anderen Gründen angeführtes Dokument

& Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument

EPO FORM 1503 03.82 (P04C03)

ANHANG ZUM EUROPÄISCHEN RECHERCHENBERICHT ÜBER DIE EUROPÄISCHE PATENTANMELDUNG NR. EP 00 81 0028

In diesem Anhang sind die Mitglieder der Patentfamilien der im obengenannten europäischen Recherchenbericht angeführten Patentdokumente angegeben.
Die Angaben über die Familienmitglieder entsprechen dem Stand der Datei des Europäischen Patentamts am
Diese Angaben dienen nur zur Unterrichtung und erfolgen ohne Gewähr.

23-05-2001

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
WO 9945684 A	10-09-1999	FI 980485 A	04-09-1999
		AU 2627199 A	20-09-1999
		EP 1060594 A	20-12-2000

EPO FORM P0461

Für nähere Einzelheiten zu diesem Anhang : siehe Amtsblatt des Europäischen Patentamts, Nr 12/82